様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　１３　日現在

機関番号：　１７１０２
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2015
課題番号：　２５３３０１３１

研究課題名（和文）多種類サイバー攻撃の高速検知のためのヒストグラムデータベースの応用研究

研究課題名（英文）Effective detection of various kinds of cyberattacks using histogram database technology

研究代表者

馮　尭楷（Feng, Yaokai）

九州大学・システム情報科学研究科（研究院・助教

研究者番号：６０３６３３８９

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：１）多種類のサイバー攻撃を検知するための特徴量を決定し、機械学習を利用して検知性能を確認した。具体的に言えば、DRDoS攻撃、DNSアンプ攻撃、DDoS攻撃の予兆およびポートスキャンの検知でした。
２）既存に収集したサイバー攻撃の挙動を更に詳しく分析する上で、検知するための必要なヒストグラムの構成法および通常時挙動モードの抽出法を詳細的に検討して、その性能も実証した。
３）大規模多次元のパケット流れからヒストグラムを動的高速に構築する方法を考案して、その性能を確認した。

研究成果の概要（英文）：1) For detecting many kinds of cyber attacks, features and machine learning algorithms were tested and their detection performance was verified. Specifically, DRDoS attacks, DNS amp attacks, the sign of DDoS attacks.　2) Histogram construction method was investigated by further detailed analysis of the behavior of the cyber attacks that have been collected. The performance was also demonstrated.　　3) In order to dynamically and rapidly construct histogram in real time from large, multidimensional packet datasets was invesitgated.
To accomplish an effective and rapid abnormality detection system, it is necessary to construct dynamically a moving histogram at high speed. We developed a method to incrementally construct histograms.

研究分野：　ネットワークセキュリティ

キーワード：　分散型攻撃　挙動に基づく異常検知　サイバーセキュリティ　ポートスキャン攻撃

１．研究開始当初の背景

インターネットの普及・拡大に伴い、サイバーテロという言葉があふれるほど、インターネットに接続されたシステムに対する不正侵入の種類と頻度も増加している。不正侵入には、サーバへ侵入してデータの改竄や窃盗を行うもの、サーバやネットワーク機器に高い負荷を与えてサービス停止に追い込むもの、システムに侵入して他のシステムへの新たな攻撃の踏み台にするものなど、重大な影響を与えるものが多い。例えば、2011 年は、国内の大手重工メーカや衆議院・参議院がサイバー攻撃を受け、世間の注目を集めた。政府も企業も巨大な資金を投入し、多くの研究者が様々な検知案を研究・構築しているが、サイバー攻撃が減少する様子は一向にみられない。その原因としては、１）攻撃の技術が進化・多様化していること、及び２）既存の検知手法が完全ではなく開発途上にあること、が挙げられる。

２．研究の目的

本研究では既存の案と全く違う方法で、トラフィック特徴量ヒストグラムデータベースによる、多種類のサイバー攻撃を対応できる高速的かつ有効な検知手法の提案および検証を行う。この新たな手法を提案する背景には、申請者が総務省「サイバー攻撃情報の類似性・局所性・時系列性解析技術」に関するプロジェクトの一環として行った最近の研究・成果が挙げられる。すなわち、大量のパケットトラフィックから、その特徴量（始点 IP アドレスなど）のヒストグラムを用いて通常時の挙動モードを推定し、それを利用する攻撃検知の方法は、既存方法で検知困難な低レート攻撃および次世代の攻撃とも呼ばれている「分散型スキャン攻撃」に関して、極めて有効であることが示された。従って、ネットワーク攻撃は、大量学習用パケットトラフィックデータから、統計的特徴量を抽出・ヒストグラム化して解析することで、異常検知を行えることを確認する。

３．研究の方法

本研究は、代表者のほかに修士２人との３人のグループで行った。本申請課題を実現するために、第１段階では、各種類の攻撃を有効検知するためのヒストグラムの構成法および通常時挙動モードの抽出法を検討した。これらは本申請課題の基礎部分である。第２段階では、動的なヒストグラムの高速な構築アルゴリズムを開発した。その後は、多種類の異常検知の機能を定量的に評価した。第３段階では、本システムに相応しい索引技術を導入して、異常検知をさらに高速化させた。複雑なヒストグラムを多次元空間への配置、次元数の縮約、有効な距離関数、インデックシング技術、高速検索アルゴリズムなどを開発した。

４．研究成果

挙動に基づくポートスキャンの検知の核心は学習アルゴリズムである。既存の学習アルゴリズムこのアルゴリズムの問題点として、2 つのパラメータが必要であり、その決め方はデータ依存であり一定不変のものではないので、専門家にとっても決定が難しいことである。本研究では、この問題を解決するためにパラメータなしの新しい学習アルゴリズムを提案した。

1. パラメータなしの学習アルゴリズムの提案

本提案の学習アルゴリズムは既に我々の先行研究で紹介された。その発展として、本論文では提案学習アルゴリズムの学習性能を評価し、ポートスキャン検知に応用する際の検知性能を具体的に検証する。

提案の学習アルゴリズムの目的は度数分布からパラメータを用いず通常モードを自動的に抽出することである。2 章で述べたように本研究では垂直ポートスキャンの検知を取り上げる。垂直ポートスキャンの場合は、多くのポートがアクセスされると考えられる。即ち、垂直ポートスキャンのトラフィックは度数分布の右側に、通常モードのトラフィックは左側に集まることになる。そのため、度数分布図の両側から内側へすべての bin をチェックしながら通常 bin-group と異常 bin-group を区別できれば学習結果が得られる。ここで bin-group は度数分布の中で zero-bin（高さが zero である bin）により分けられた bin の集合を指す。本提案の学習アルゴリズムは 2 つのポインターを度数分布の両側に設置し、各々を内側に向かって移動させ、出会った点を学習結果とする。

本論文で提案する学習アルゴリズムの概要は表 3（初期化部分）と図 5（主体部分）に示すとおりである。すべての bin は幾つかの zero-bin によって分割されていると仮定する。ただ一つの bin-group しか存在しない場合は、このような bin-group をすべて正常トラフィックと仮定し、この bin-group の右端を学習結果とする。bin-group の面積はその bin-group に含まれる bin の度数（高さ）の合計を意味する。

提案する学習アルゴリズムは、Right_Pointer と Left_Pointer という二つのポインターを利用する。最初、Right_Pointer は一番右側の bin-group の右端に置き、異常な bin-group を調べる目的で利用する。一方 Left_Pointer は一番左側の bin-group の右端に置き、通常な bin-group を調べる目的で利用する。Left_Pointer はある条件（条件 1）によって左から右へ bin-group ごとに進む。Right_Pointer は別の条件（条件 2）によって右から左へ bin-group ごとに進む。この二つのポインタ

ーとその移動条件を導入することにより、本研究では学習アルゴリズムの自動化を実現することができた。この二つのポインターは一致するまで繰り返して移動させ、一致したところを学習結果とする。もし二つのポインターが一致する前に、両方も止まったら、in-group の合併を行う。Bin-group の合併を用いることで、2 つのポインターが必ず一致にすることを保証できる。

ここで Dist_left は Right_Pointer とその左に隣接する bin-group との距離であり、Span は横軸にある最左端の bin と最右端の bin との距離である。Area_left は Right_Pointer の左に隣接する bin-group の面積であり、Total_area はすべての bin の度数（縦軸の値）の和である。この条件は Right_Pointer の左側にある bin-group は異常か否かを判別するために、その bin-group の面積割合と、その bin-group からその bin-group の左に隣接する bin-group までの距離割合を用いる。面積の割合は小さいほど、且つ距離の割合が大きいほど、異常と判別される可能性が高くなる。

Left_Pointer の移動条件は次の通りである。

ここで Dist_right は Left_Pointer とその右に隣接する bin-group との距離であり、Area_ right は Left_ Pointer の右に隣接する bin-group の面積である。この条件は、Left_ Pointer の右側の bin-group が通常か否かを判別するために、その bin-group の面積割合と、その bin-group とその bin-group の右に隣接する bin-group の距離割合を用いる。面積の割合は大きいほど、且つ距離の割合が小さいほど、通常と判別される可能性が高くなる。

二つのポインターが一致した場合、その地点を学習結果として採用する。一方、二つのポインターが一致する前に止まった場合、Right_Pointer 左側にある二つの bin-group を合併させる。その後、再び二つのポインターの移動条件を適用し移動を繰り返す。この学習アルゴリズムは必ず二つのポインターが一致して終了することを 4。5 節で説明する。

bin-group の合併を行った後、この学習アルゴリズムはポインターの移動を繰り返して実行する。bin-group の合併が発生する最悪の場合を考えると、この時、二つのポインターの間に一つの bin-group しか存在しない。この時、Dist_left と Dist_right、Area_left と Area_right は等しくなる。従って、Right_Pointer また Left_Pointer のどちらは必ず移動する。なぜなら、二つのポインターの移動条件は逆になっているからである。その結果、二つのポインターは一致してアルゴリズムは終了する。

2. 性能実証

提案手法では、学習アルゴリズムを適用する前に度数分布を作成する必要がある。そのためには、時間単位と bin 幅を決める必要がある。この章では、まず、同じデータセットに対して作成した異なる度数分布がどのように学習の結果に影響するかを調査する。そして、学習アルゴリズムの検知性能を検証する。度数分布図の学習結果への影響を検証する。本論文では、データ量の多いダークネットから収集されたデータを用いる。このデータは異常データを明示するラベル付きの ground-truth データがないため、本提案の検知結果を評価することは難しい。

提案アルゴリズムを適用する度数分布図を作成するためには、時間単位と bin 幅を決める必要がある。時間単位はトラフィックを集計する最小時間幅として、異常に対する検知の速さと直接に関連する。具体的に言えば、時間単位が長くなると異常検知は遅れ、短すぎると通常モードが少なくなり検知システムは異常に対する過敏症状が出る。適切な bin 幅は、必要な通常モードの抽出精度によって変わる。本節では、時間単位と bin 幅が及ぼす学習結果への影響を調べる。なお、時間単位と bin 幅は度数分布を作成する際のパラメータであるため、本提案の学習アルゴリズムのパラメータではない。

一般的に、実際のトラフィックデータを収集することは難しい。一方、多くの研究が、ダークネットデータの有効性を示している。ダークネットとはインターネット上にある未使用な IP アドレスからなるネットワークである。このダークネットデータを使ったスキャン検知の研究は数多く存在している。そこで、我々の実験もダークネットデータを使って提案アルゴリズムの性能を検証する。今回の実験は独立行政法人情報通信研究機構（NICT）から提供されたダークネット観測データ [5-A1]（2011 年 6 月、30 日間約 8799 万 TCP パケット）を利用する。

本実験では、時間単位として 10 分、30 分、60 分の 3 種類を、bin 幅として 250、500、750、1000、2000、3000 の 6 種類を設定した。実験結果によると bin 幅は実験結果に大きく影響を与えていない。このため、ここでは 500 と 1000 を bin 幅の例として挙げる。

図 1 によると、時間単位を 30 分間隔とし、bin 幅を 1000 とした場合、学習結果は 44 番目の bin のところとなっている。即ち、学習結果として、通常モードは 44×500（bin 幅）= 22000 になる。図 7 は、時間単位は同じく 10 分間隔で､bin 幅を 1000 とした場合である。この時、通常時モードは 22×1000（bin 幅）=

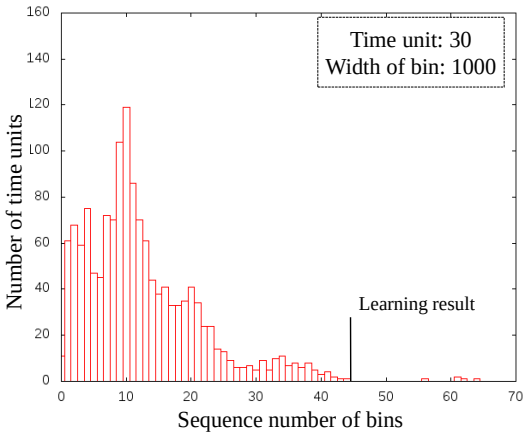

図 1　度数分布図: 時間単位=30 分、bin 幅=1000

22000 となっていた。時間単位が比較的小さいため度数分布図全体が左に寄っていることが分かる。 この実験結果により、次の考察が得られる。

時間単位が増えると、通常モードの範囲は大きくなる傾向がある。その原因は時間単位内にアクセスされたポート数は大きくなるからである。

ある時間単位において、bin 幅を変えても学習結果に大きな影響はない。

異常トラフィックの学習結果への影響：

異常トラフィックの検知実験に用いたデータは、当研究室のサーバで収集されたものに攻撃データを追加した人工データである。研究室ウェブページへの通信やメールなどはこのサーバを経由しているため、日常的なトラフィックが記録されている。本実験ではこのデータを正常なトラフィックとして扱う。

一方、異常データすなわち攻撃データを作るために、 Nmap を利用した。Nmap はポートスキャンや OS 検出など多くの機能を兼ね備えているソフトウェアであり、よく利用されているセキュリティスキャナである。

1)　学習データ

本実験では正常なトラフィックとして当研究室サーバ取集した 2 日間（2014 年 11 月 8 日－2014 年 11 月 9 日）のトラフィックデータ [5-A2)]（48 時間約 500MB の TCP パケット）を利用した。この通常トラフィックに異常トラフィックとして、Nmap を使って下記の 3 パターンのポートスキャン攻撃によって得たトラフィックを混ぜた。それぞれの学習結果を分析することにより、異なるポートスキャンデータの学習結果への影響を調べる。

パターン 1 は、intense scan と呼ばれるポートスキャン攻撃である。この種の攻撃は、危険性が高いポートスキャンとして、よく使われる手段の 1 つである。パターン 2 は、2 種類のポートスキャン攻撃を含んでいる。1 つは intense scan で、もう 1 つはより高速のポートスキャンである。パターン 3 では、3 種類のポートスキャン攻撃を行った。Intense scan 以外に、スキャン速度（単位時間内にスキャンしたポート数）が異なる 2 種類のポートスキャンを加えたものである。なお、同じ種類の攻撃であってももランダム性およびパラメータにより同じ攻撃データになるとは限らない。

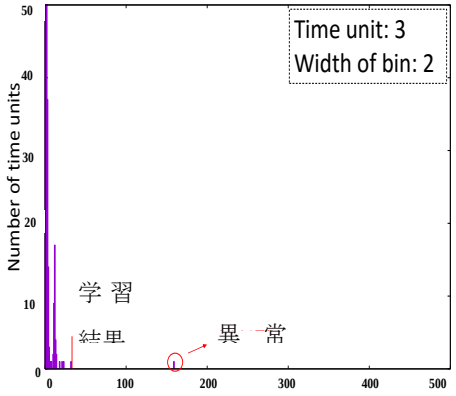

図 2　度数分布図および学習結果

2)　テストデータ

テストデータは 2 日間（2014 年 11 月 12 日－2014 年 11 月 13 日）に各 1 回のスキャン攻撃を行って収集したトラフィックデータである。 データの流れを図 15 に示す。

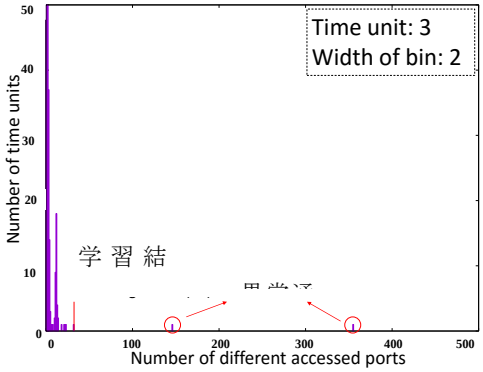

図 3　度数分布図および学習結果（パターン 2）

度数分布の作成：

前述したように、学習アルゴリズムを使う前に度数分布を作成する。 5。1 節では時間単位と bin 幅は及ぼす度数分布図への影響を論じた。今回の実験は研究室のサーバで収集した小規模のデータであるため、時間単位と bin 幅を小さい数値に設定すれば提案の学習アルゴリズムの検知性能を実証することができると考えられる。今回の実験で時間単位は 3 分間隔とし、bin 幅は 2 とした。[5-B1)]48 時間のデータであるため、960 時間単位がある。

上述した 3 つのパターンで作成した度数分布および学習の結果を図 12、図 13 および図 14 に示す。[5-C)]学習結果を示す bin は 3 つのパターンとも同じく 33 番 bin で、通常モードは 33×22（bin 幅）= 66 となった。

挙動に基づく検知手法を利用した関連研究の FHST 手法を紹介した。本節では図 12～14 の人工データを使って FHST 手法との学習結果の比較を行う。FHST アルゴリズムを使うにはパラメータを決める必要があるため、本論文では 9 組のパラメータを試した。比較結果は表 4 に示す。この比較の結果からは次のことが分かる。

既存手法では学習に失敗することがあった。本実験では、パラメータが α= 0。3、 β= 0。3 の時、FHST 手法の学習結果を示す bin は 269 番の bin になった。bin 幅が 2 であることから通常モードは 538 である。即ち、図 14 における左から 1 番目と 2 番目の異常トラフィックグループを通常と判断してしまっていた。なぜなら、 図 14 にある三つの異常の中、左側 2 つの異常間の距離は、横軸全体の 20%より大きいが 30%より小さい。そのため、α を 0。2 とするか 0。3 とするかによって結果は大きく変わった。この学習結果を通常モードとして利用すれば、明らかに異常の検知漏れが多く生じることになる。

従って、本提案は学習性能を犠牲せず学習の自動化を実現したといえる。

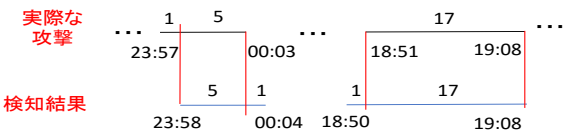

図 4　実際な攻撃と検知の結果

パターン 3 の実験（図 14）に用いたデータ約 500MB を利用して本提案手法と FHST 手法の実行時間を比較した。両手法は度数分布図の作成までは全く同じプロセスで、学習アルゴリズムのみが異なっている。実験には、 Core i7 4960k の CPU と 8GB のメモリを持つサーバ上で動作する仮想マシンを利用した。度数分布図の作成を含めて学習の結果が得るまで、両手法とも 10 秒弱の時間を要した。学習段階のみを見れば、両手法の所要時間は FHST 手法 0。6ms に対して、本提案手法 0。9ms であった。これにより、学習段階の所要時間は、両手法が同じである度数分布の作成時間に比べて無視できるほどである。

データ量が大きくなっても、学習アルゴリズムの実行時間は Bin の数と Bin の分布にのみ依存するため、学習トラフィックデータのサイズには依存しない。なお、度数分布の作成には、全てのデータを 1 回走査必要があるため、全体では実行時間はデータ量 n に対して O(n)の関係にある。

これまでの実験では、トラフィックデータの変化と学習結果への影響を調べた。本節では、学習で得られた通常モード 66（表 4 を参照）を図 15 で示したテストデータに含まれる異常トラフィックを検知してみることにより、本論文で提案した学習アルゴリズムの有効性を検証する。本実験では 1 分間を最小単位とし、検知率などを計る。検知結果は図 16 と表

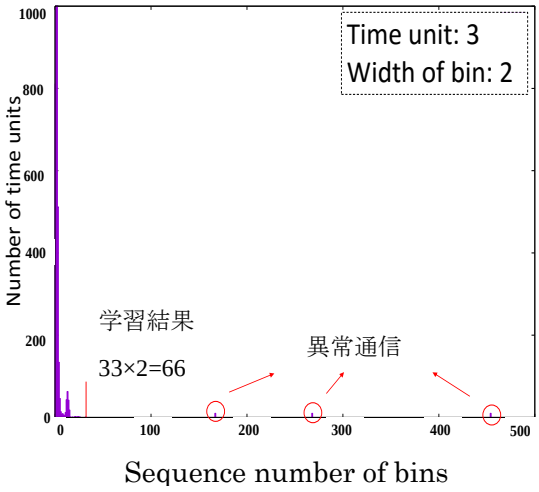

図 5 拡大したデータの度数分布と学習結果（ケース 1）

5 で示す。

実験結果によれば、提案の学習アルゴリズムによる学習結果をポートスキャン検知に用いれば、95%以上の検知率を達成した。なお、[5-D)]FHST 手法の学習結果は最良のパラメータを選択した場合、本提案の結果と同じであるため、検知性能も同じである。従って、パラメータチューニングが必要ない本論文の提案手法も同等の良い検知結果を得たといえる。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 1 件）

○王サン，フォン　ヤオカイ，川本 淳平，堀　彰良，櫻井 幸一，
挙動に基づくポートスキャン検知の自動化に向けた学習アルゴリズムの提案とその性

能評価,
情報処理学会論文誌, 56, 9, 1770, 1781, 2015.09.

〔学会発表〕(計 10 件)
① Yaokai Feng, Yoshiaki Hori, Kouichi Sakurai,
A Proposal for Detecting Distributed Cyber-Attacks Using Automatic Thresholding,
the 10th Asia Conference on information security, IEEE CPS, 152, 159, 2015.05.

② Can Wang, Yaokai Feng, Junpei Kawamoto, Yoshiaki Hori, Kouichi Sakurai,
A Parameterless Learning Algorithm for Behavior-Based Attack Detection,
9th Asia Conference on information security, 2014.09.

③ 呂 良, フォン ヤオカイ, 川本 淳平, 櫻井 幸一,
ランダムフォレストを用いたボットネットの検出,
電子情報通信学会総合大会, 2016.03.16.

④ 高 宇軒, フォン ヤオカイ, 川本 淳平, 櫻井 幸一,
機械学習を利用した DRDoS 攻撃検知の提案とその性能実証,
第 33 回 暗号と情報セキュリティシンポジウム(SCIS2016), 2016.01.22.

⑤ 李 鵬飛, フォン ヤオカイ, 川本 淳平, 櫻井 幸一,
パケットマーキングとロギングを用いたサイバー攻撃に対するトレースバック,
コンピュータセキュリティシンポジウム 2015 (CSS2015), 2015.10.23.

⑥ フォン ヤオカイ, 堀良彰, 櫻井 幸一,
A Behavior-based Engine for Detecting Distributed Internet Attacks and its Performance Investigation,
第 32 回 暗号と情報セキュリティシンポジウム(SCIS2015), 2015.01.20.

⑦ 蔡龍洙, フォン ヤオカイ, 川本 淳平, 櫻井 幸一,
挙動に基づく DNS アンプ攻撃の検知,
コンピュータセキュリティシンポジウム 2015 (CSS2015), 2015.10.22.

⑧ 王サン, フォン ヤオカイ, 川本 淳平, 堀良彰, 櫻井 幸一,
挙動に基づくポートスキャン検知手法に向けたパラメータなしの学習アルゴリズムの提案とその性能評価,
第 32 回 暗号と情報セキュリティシンポジウム(SCIS2015), 2015.01.20.

⑨ Yaokai Feng, Yoshiaki Hori, Kouichi Sakurai,
An Approach for Detecting Distributed Cyber-Attacks,
The 8th Workshop WAIS2015 (Soul), 2015.01.09.

⑩ Can Wang, Yaokai Feng, Junpei Kawamoto, Yoshiaki Hori, Kouichi Sakurai,
A Learning Algorithm for the Threshold in Behavior-based PortScan Detection and Its Evaluation,
The 8th Workshop WAIS2015 (Soul), 2015.01.09.

〔図書〕(計 0 件)

〔産業財産権〕
○出願状況 (計 0 件)

名称:
発明者:
権利者:
種類:
番号:
出願年月日:
国内外の別:

○取得状況 (計 0 件)

名称:
発明者:
権利者:
種類:
番号:
取得年月日:
国内外の別:

〔その他〕
ホームページ等

６. 研究組織
(1)研究代表者
フォン ヤオカイ (Feng Yaokai)
九州大学・システム情報科学研究院・助教

研究者番号:60363389

(2)研究分担者
( )

研究者番号:

(3)連携研究者
( )

研究者番号: